Exercises workshop

START SECURITY TESTING WITH THE TOOLS YOU ALREADY USE!

Jeroen Willemsen & Nanne Baars

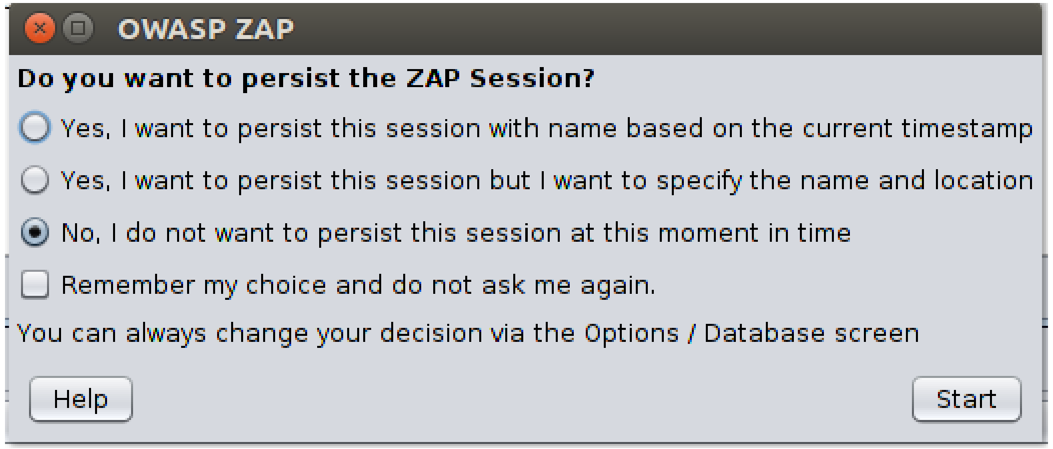
Exercise 1 – Familiarize with ZAP

- Open a terminal and in the `~/workspace/NodeGoat/`
  - Type: `npm start`
  - When it fails to start: open a new terminal and type `mongod`

- Open another terminal, start ZAP in the directory: `~/tools/ZAP_2.6.0`
  - Type: `./zap.sh`

Exercise 1 – Familiarize with ZAP

- When you open ZAP you will see the following windows:



Do you want to persist the ZAP Session?

○ Yes, I want to persist this session with name based on the current timestamp

○ Yes, I want to persist this session but I want to specify the name and location

● No, I do not want to persist this session at this moment in time

□ Remember my choice and do not ask me again.

You can always change your decision via the Options / Database screen

- Can be helpful when you want to save request/responses when performing a test.

Exercise 1 – Familiarize with ZAP

- In the “URL to attack” box type: `http://localhost:4000`
- Check the results of the automated scan, do you see some interesting findings?
- Look at the request/response for one of the findings
- What happens if you change the “Attack mode” within ZAP?
- Is Node Goat failing? Try restarting it!

Exercise 2 - Browse the website

- Register or login:
  - Admin Account - u:admin p:Admin_123
  - User Accounts (u:user1 p:User1_123), (u:user2 p:User2_123)
- Login and browse the site.
- Take a look at ZAP.
- Questions:
  - Do you see more alerts?
  - If you perform an attack again do you see more alerts?
  - Can you validate these alerts?

Exercise 3 – Automated test cases

- The tests are located in the `~/workspace/NodeGoat/test/e2etest` folder.
- ZAP:
  - Start ZAP.
  - Open Tools → Options → API and disable the API key.

Exercise 3 – Automated test cases

- In `~/workspace/NodeGoat`
  - Type: “npm run test:e2e” to run the tests.
- Add more test cases and look at ZAP:
  - For example write a test case for clicking on “Learning Resources”.
  - Write a test case to update your profile.
- Need to reset the db? Use
  - Type: `npm run db:seed`

Bonus exercise

- In `~/workspace/Nodegoat/test/security` you will find a file called `profile-test.js.bak`
  - Rename this to `profile-test.js.`
- Make sure you have configured your zap and `~/workspace/NodeGoat/config/env/development.js` correctly.
- In `~/workspace/NodeGoat,`
  - Type: npm run test:security
- When it is finished, you can find the test results in the test directory.

Bonus exercise

- Now, open profile-test.js and take a look!
  - Try to understand what it does, given the UI exercises that we have done.
  - You can apply this to your own projects as well!
- See https://github.com/zaproxy/zaproxy/wiki/ApiDetails for more details.